

RECEIVED
CENTRAL FAX CENTER

SEP 19 2007

REMARKSI. Introduction

In response to the Office Action dated April 19, 2007, claims 1, 17, 30 and 46 have been amended. Claims 1-58 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Non-Art Rejections

In paragraph (2) of the Office Action, claims 17 and 46 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite due to a lack of antecedent basis for the phrase "secondary data."

Applicant's attorney respectfully traverses this rejection, by noting that the phrase "secondary data" is properly introduced in claims 17 and 46, which provides the antecedent basis.

III. Statutory Subject Matter Rejections

In paragraph (3) of the Office Action, claims 1-58 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Applicant's attorney has amended claims 1, 17, 30 and 46 to overcome this rejection, by reciting that the signal generated pertaining to the comparison of the second processed data to the first processed data is provided "for use in an authentication process." Applicant's attorney submits that this limitation provides a tangible result that is generic to the alternatives listed, for example, in dependent claims 11-15.

However, should issues still remain in this regard, Applicants' attorney requests that the Examiner indicate how the rejection can be overcome, in accordance with the directives of the Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility (Interim Guidelines) II. Specifically, should it be necessary, the Applicants' attorney requests that the Examiner identify features of the invention that would render the claimed subject matter statutory if recited in the claim. See Interim Guidelines IV.B, as well as M.P.E.P. § 2106.

IV. Prior Art RejectionsA. The Office Action Rejections

In paragraphs (4)-(5) of the Office Action, claims 1-58 were rejected under 35 U.S.C. §102 as being anticipated by Musgrave et al., U.S. Patent No. 6,202,151 B1 (Musgrave).

Applicant's attorney respectfully traverses these rejections.

B. Applicant's Invention

Applicant's invention, as recited in independent claims 1, 17, 30 and 46, is generally directed to processing data to enable the authorized submission and authentication of biometric data in a confidential manner. Claim 1, as amended, is representative, and recites:

- receiving a first biometric data and a first personal key;
- processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a first processed data;
- receiving a second biometric data and a second personal key;
- processing the second biometric data combined with the second personal key through the irreversible cryptographic algorithm to form a second processed data;
- eliminating all storage or trace of the first and second biometric data and personal keys in an unprocessed form;
- comparing the second processed data to the first processed data, without accessing the first and second processed data in an unprocessed form, in order to enable authentication of the first and second biometric data and personal keys in a confidential manner; and
- generating a signal pertaining to the comparison of the second processed data to the first processed data for use in an authentication process.

C. The Musgrave Reference

Musgrave describes a technique for combining biometric identification with digital certificates for electronic authentication called biometric certificates. The technique includes the management of biometric certificates through the use of a biometric certificate management system. Biometric certificates may be used in any electronic transaction requiring authentication of the participants. Biometric data is pre-stored in a biometric database of the biometric certificate management system by receiving data corresponding to physical characteristics of registered users through a biometric input device. Subsequent transactions to be conducted over a network have biometric certificates generated from the physical characteristics of a current user, which is then appended to the transaction, and which then authenticates the user by comparison against the pre-stored biometric data of the physical characteristics of users in the biometric database.

D. The Applicant's Invention is Patentable Over the References

Applicant's claimed invention is patentable over the references, because the claims contain limitations not taught by the reference. Specifically, Applicant's invention is designed to enable the authorized submission and authentication of biometric data in a confidential manner. In this regard, the biometric data is processed by an irreversible cryptographic algorithm causing the resulting data to be undecipherable, irreversible and undecryptable, but still capable of being used for comparison purposes. Moreover, all traces of the unprocessed biometric data are eliminated from the system and storage.

The Office Action, on the other hand, asserts that Musgrave describes all the limitations of Applicant's independent claims:

5. Claims 1-58 are rejected under 35 U.S.C. 102(b) as being anticipated by Musgrave et al. (U.S. Patent No. 6,202,151 B1), as provided by the applicant.

C1. A method for processing data comprising: receiving a first biometric data and a first personal key; processing the first biometric data and the first personal key through an irreversible cryptographic algorithm to form a first processed data; receiving a second biometric data and a second personal key; processing the second biometric data and the second personal key through the irreversible cryptographic algorithm to form a second processed data; comparing the second processed data to the first processed data; and generating a signal pertaining to the comparison of the second processed data to the first processed data. (Column 3, lines 57-60, column 2, lines 26-29 and lines 53-65, column 5, lines 15-22, and Figure 3. Please note "one-way hashing function" is, by its definition, 'irreversible.' Although Musgrave et al. teach using an "inverse 45 of the hash function 34, (Col. 5, lines 39-41)," Musgrave et al. have alternatively taught the use of non-invertible/reversible hash/one-way function in paragraph 2 of column 5. Please see applicant's disclosure, paragraph 0008, for verification.)

Applicant's attorney disagrees with this analysis.

Musgrave merely describes user authentication (proving a user is who they say they are) using biometric data that is transmitted in a secure manner involving public and private keys. Consider, for example, the following portions of Musgrave

Col. 4, line 47 – col. 6, line 17

The disclosed biometric certification system 24 is shown in FIGS. 3-4. It has a set of input devices, including a biometric input device 26, a user data input device 28, and a transaction data input device 30. The biometric input device 26 generates first biometric data from the physical characteristics of the user, such as fingerprints, hand geometry, iris and retinal appearance, and speech patterns.

The biometric input device 26 may include visual cameras and/or other visual readers to input fingerprints, hand geometry, iris appearance, and retinal

appearance. For example, companies such as IDENTIX, FUJITSU, and AUTHENTEC provide such equipment for reading fingerprints, while RECOGNITION SYSTEMS provides equipment to read hand geometry. EYE-IDENTIFY is an example of a company which provides retinal imaging devices, while IRISCAN and SENSAR are examples of companies which provide iris imaging devices.

Alternatively, the biometric input device 26 may be adapted to receive audio characteristics of a user. For example, a microphone in conjunction with a speech digitizer may be used to receive and digitize speech. Such companies as BBN, T-NETIX, and ALPHA-TEL provide such equipment for receiving and digitizing speech to generate corresponding biometric data.

Biometric input devices known in the art may be used to receive other physical characteristics such as facial and body appearance via, for example, a camera, as well as the genetic composition of the user by means of genetic material gathering procedures, such as blood lancets.

The biometric certificate as shown in FIG. 2 may be generated by concatenating transaction data, a public key, and the set 16 of data, including the biometric data 20, using a first concatenator 32, which may be embodied as an adder. The transaction data is received from the transaction data input device 30 corresponding to the electronic transaction such as an electronic funds transfer. The set 16 of data is input through the user data input device 28 which may be in a sequence, as shown in FIG. 2, and which may include a unique subject ID 18 corresponding to the subject; that is, the individual or entity such as a corporation, having the public key. The set 16 of data also includes various other fields described above with respect to FIG. 1.

The biometric data 20 is obtained directly from the physical characteristics of the subject through the biometric input device 26. The unique subject ID 18 of the user may include M bits, in which typically $M \approx 50$ bits ≈ 6 bytes or less, while the biometric data 20 typically includes much more data than the unique subject ID 18. Generally, the biometric data 20 has N bits in which N is about 64 bits or more; that is, about 6 bytes or more. In fact, the amount of the biometric data 20 is unlimited; for example, a fingerprint may be visually scanned to any resolution to obtain key fingerprint aspects which uniquely distinguish fingerprints, or alternatively to obtain data representing pixels of the entire fingerprint. Accordingly, the biometric data 20 may require large amounts of memory for storage such as 2 kB or even 4 MB. Accordingly, in the preferred embodiment, N is much greater than M .

The authenticating certificate, being the concatenation of the set 16 of data, including the biometric data 20, with the public key and the transaction data, is then processed, for example, using a hash function 34, such as a one-way hashing function, to generate a hashed value. RSA and SHA-1 are examples of public key cryptographic methods and one-way hashing which may be used for such encryption and hashing functions. The RSA method is described, for example, in U.S. Pat. No. 4,405,829 to Rivest et al., which is incorporated herein by reference. The SHA-1 method is described, for example, in U.S. Pat. No. 5,623,545 to Childs et al., which is incorporated herein by reference.

The hashed value is then sent to a registration authority (RA) 36 having a biometric certificate generator 38, in which the hashed value is signed; that is, encrypted, using the private key of the user to generate a digital signature 22,

incorporating the biometric data 20. Using a second concatenator 40, which may be an adder circuit, the digital signature 22 is then appended to the transaction data from the transaction data input device 30 for transmission over, for example, a network 42 or the Internet.

Referring to FIG. 4, after receiving the electronic transaction from the network 42, a receiver 44 decrypts the electronic transaction using its private key, de-hashes the decrypted electronic transaction using an inverse 45 of the hash function 34, and extracts the biometric certificate 46 from the de-hashed data using a biometric certificate extractor 46, which may be an adder or a subtractor circuit for separating the biometric certificate from the rest of the data.

The receiver 44 then sends the biometric certificate to a biometric certificate management system (BCMS) 48 for authentication thereof. The BCMS includes a biometric data extractor 50 which extracts the first biometric data from the biometric certificate. The biometric data extractor 50 may be an adder or a subtractor circuit, which then applies to a classifier 52 the first biometric data allegedly corresponding (before authentication) to the user.

The BCMS 48 also accesses a biometric database 54 to obtain pre-stored biometric data from registered users identified by the user data, such as the unique subject ID 18 provided in the biometric certificate 20. After obtaining second biometric data corresponding to the user, the BCMS 48 applies the second biometric data to the classifier 52 for classification with respect to the first biometric data.

The classifier 52 may be a comparator, or alternatively a software routine or other hardware/software devices implementing data matching techniques, for comparing the biometric data to obtain a decision value. Alternatively, the classifier 52 may be a trained neural network 53 and/or a fuzzy logic classifier for classifying whether or not, within an error tolerance, the first and second biometric data were obtained from the same individual using biometric input devices. Such classification methods for authentication of images and data sequences using neural networks are described, for example, in U.S. Pat. No. 5,619,620 to Eccles, which is incorporated herein by reference.

The classifier 52 then generates an authentication decision, which may be logic values corresponding to YES or NO, or TRUE or FALSE, indicating verification of the authenticity of the user sending the electronic transaction. Alternatively, the authentication decision may be a numerical value, for example, corresponding to a percentage of confidence of authenticity.

The receiver 44 then responds to the authentication decision to process the electronic transaction; for example, an electronic funds transfer. The receiver 44 may include a predetermined threshold of, for example, 98% authenticity, to be exceeded in order to proceed with the processing of the electronic transaction.

The above portions of Musgrave describe the biometric data being extracted from a de-hashed biometric certificate for comparison with pre-stored biometric data from registered users. Consequently, the system of Musgrave recovers the biometric data in a decrypted form for use in performing the comparison.

CENTRAL FAX CENTER

SEP 19 2007

Applicant's invention, on the other hand, does not allow recovery of the biometric data and personal key in its unprocessed (decrypted) form. Instead, Applicant's invention is directed to protecting the biometric data and personal key from being captured and revealed (a) while in transit to a central function for comparison; (b) while stored in a database for future use the in the comparisons; and (c) during the comparison itself by the central function. In this regard, Applicant's invention eliminates all storage and traces of the biometric data and personal key after they are irreversibly encrypted.

Musgrave's use of the unencrypted biometric data for comparison and storage of the unencrypted biometric data presents an opportunity for leakage (stolen, misused data). Applicant's invention, on the other hand, uses and stores only the encrypted biometric data and personal key, i.e., the biometric data and personal key are used only in a processed (anonymized) form.

Thus, Applicant's attorney submits that independent claims 1, 17, 30 and 46 are patentable over Musgrave. Further, dependent claims 2-16, 18-29, 31-45 and 47-58 are submitted to be patentable over Musgrave in the same manner, because they are dependent on independent claims 1, 17, 30 and 46, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-16, 18-29, 31-45 and 47-58 recite additional novel elements not shown by Musgrave.

V. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited.

Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicant's undersigned attorney.

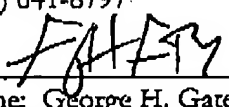
Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: September 19, 2007

GHG/

By: 
Name: George H. Gates
Reg. No.: 33,500

G&C 30571.302-US-U1